

LDPC coded transmissions over the Gaussian broadcast channel with confidential messages

Marco Baldi, Nicola Maturo, Giacomo Ricciutelli, Franco Chiaraluce,
DII, Università Politecnica delle Marche,
Ancona, Italy

Email: {m.baldi, n.maturo, f.chiaraluce}@univpm.it, g.ricciutelli@gmail.com

Abstract—We design and assess some practical low-density parity-check (LDPC) coded transmission schemes for the Gaussian broadcast channel with confidential messages (BCC). This channel model is different from the classical wiretap channel model as the unauthorized receiver (Eve) must be able to decode some part of the information. Hence, the reliability and security targets are different from those of the wiretap channel. In order to design and assess practical coding schemes, we use the error rate as a metric of the performance achieved by the authorized receiver (Bob) and the unauthorized receiver (Eve). We study the system feasibility, and show that two different levels of protection against noise are required on the public and the secret messages. This can be achieved in two ways: i) by using LDPC codes with unequal error protection (UEP) of the transmitted information bits or ii) by using two classical non-UEP LDPC codes with different rates. We compare these two approaches and show that, for the considered examples, the solution exploiting UEP LDPC codes is more efficient than that using non-UEP LDPC codes.

Index Terms—Broadcast channel with confidential messages, low-density parity-check codes, physical layer security, unequal error protection.

I. INTRODUCTION

The BCC [1] is a well-known transmission model for communications achieving security at the physical layer, which generalizes Wyner's wiretap channel model [2]. Since its introduction, a lot of work has been done to study the BCC from the information theory standpoint, mostly aimed at computing the secrecy capacity regions for this channel and its several variants (see [3]–[5] and the references therein). More recently, the secrecy capacity regions have been studied also for the BCC with multiple-input multiple-output (MIMO) [6]–[8] and cooperative communications [9].

For the classical wiretap channel, the use of several practical families of codes has already been investigated: this is the case of lattice codes [10], polar codes [11] and LDPC codes [12]. Instead, for the BCC, despite the large amount of theoretical work, there is still a lack of practical systems able to achieve some specific security and reliability targets. The use of coding is recognized as an important tool also in such a context, but most studies consider the abstraction of random coding [13], which indeed is difficult to translate into a practical coding scheme. At the authors' best knowledge, the only proposal of using a family of practical codes over this special channel appeared very recently in [14], and exploits polar codes. Other,

and even more widespread families of codes, like LDPC codes, have never been considered in such a context.

In this paper, we focus on the Gaussian BCC and study some practical LDPC coded transmission schemes for achieving reliability and security over this channel. For this purpose, we follow some recent literature and use the error rate as a metric [12], [15]–[18]. We define suitable reliability and security targets for the Gaussian BCC in terms of the error rate, and redefine the concept of *security gap*, defined for the Gaussian wiretap channel as the quality ratio between Bob's and Eve's channels needed to achieve the reliability and security targets.

We consider LDPC codes, since they are state-of-the-art codes able to approach the channel capacity under iterative decoding. We show that, in order to achieve transmission reliability and security over the BCC, a coding scheme with two different levels of protection against noise is needed. For this reason, we consider an LDPC code with UEP capability, and compare its performance with that achievable by using two different non-UEP LDPC codes.

The organization of the paper is as follows: in Section II we define the system model and the metrics adopted. In Section III we study the use of single codes with different rates. In Section IV we introduce UEP LDPC codes into the system. In Section V we assess the performance achievable through the considered codes and Section VI concludes the paper.

II. SYSTEM MODEL

In the Gaussian BCC, we have one transmitter (Alice) sending broadcast and confidential information over the channel. Bob is able to decode the whole information, while Eve is able to get only the public message, ideally without gathering any useful information on the secret message. Both the Alice-Bob and the Alice-Eve channels are supposed to be Gaussian.

We assume that each transmitted message is formed by n bits and includes a public and a confidential part. We also suppose to use coding, and that each transmitted message contains k information bits and $r = n - k$ redundancy bits. It follows that the overall code rate is $R = \frac{k}{n}$, and R also coincides with the overall information rate, expressed in bits per channel use, under the hypothesis of binary phase shift keying (BPSK) modulation. In our model, each transmitted message contains a block of $k_s \leq k$ information bits which are secret, while the remaining $k_p = k - k_s$ information bits form a block of public information. It follows that the secret

This work was supported in part by the MIUR project "ESCAPADE" (Grant RBFR105NLC) under the "FIRB – Futuro in Ricerca 2010" funding program.

and public information rates are $R_s = \frac{k_s}{n}$ and $R_p = \frac{k_p}{n}$, respectively, and $R = R_s + R_p$.

Concerning the redundancy part, we can suppose that it can be split into two groups: $r_s \leq r$ redundancy bits are used to check the k_s secret information bits, while the remaining $r_p = r - r_s$ bits check the public information bits. This hypothesis will be removed when we will consider codes with UEP, in which some protection classes are defined without splitting the redundancy among them. If we assume to use two different channel codes for the secret and the public parts, their code rates are $R_c^{(s)} = \frac{k_s}{k_s + r_s}$ and $R_c^{(p)} = \frac{k_p}{k_p + r_p}$, respectively. If we define $\rho = \frac{k_s + r_s}{n}$, we have $R_s = R_c^{(s)} \rho$, $R_p = R_c^{(p)} (1 - \rho)$ and $R = R_c^{(s)} \rho + R_c^{(p)} (1 - \rho)$.

A. Reliability and security metrics

We consider that both Bob's and Eve's channels are additive white Gaussian noise (AWGN) channels or, equivalently, quasi-static fading channels (QSFCs) with channel gains $\gamma^{(B)}$ and $\gamma^{(E)}$, respectively, expressed in signal-to-noise ratio (SNR) per bit. Other channel models, like the fast fading channel, are outside the scope of this paper, and will be studied in future works. $P(\gamma)$ denotes the overall frame error rate (FER) as a function of the SNR γ , that is, the probability that, within a received frame of n bits, one or more of the k information bits are in error after decoding. Similarly, $P_s(\gamma)$ ($P_p(\gamma)$) denotes the block error rate (BLER) for the secret (public) information block, i.e., the probability that, within a received frame of n bits, one or more of the k_s (k_p) secret (public) information bits are in error after decoding. Let us fix two small threshold values, δ and η , and define the security and reliability targets in terms of the decoding error probability as follows:

$$P_p(\gamma^{(B)}) \leq \delta, \quad (1a)$$

$$P_p(\gamma^{(E)}) \leq \delta, \quad (1b)$$

$$P_s(\gamma^{(B)}) \leq \delta, \quad (1c)$$

$$P_s(\gamma^{(E)}) \geq 1 - \eta. \quad (1d)$$

Let us suppose that the public information blocks are more protected against noise than the secret information blocks. This scenario is exemplified in Fig. 1, where we suppose that the public information blocks experience a lower BLER than the secret information blocks. Conditions (1) can then be translated in terms of Bob's and Eve's SNRs, i.e., $\gamma^{(B)}$ and $\gamma^{(E)}$, respectively. More precisely, by looking at the figure, we have that conditions (1a) and (1c) become

$$\gamma^{(B)} \geq \max\{\beta_p, \beta_s\} = \beta_s, \quad (2)$$

whereas conditions (1b) and (1d) become

$$\beta_p \leq \gamma^{(E)} \leq \alpha_s. \quad (3)$$

It follows from (3) that, for the system to be feasible, we must actually ensure that the public message is more protected against noise than the secret one (this typically implies $R_c^{(p)} < R_c^{(s)}$). In fact, if the opposite occurs, since

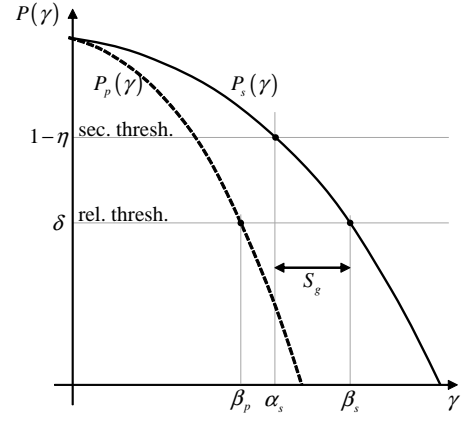


Fig. 1. Expected block error rate curves for the public and secret messages as functions of the SNR.

$1 - \eta > \delta$, we have $\alpha_s < \beta_p$, and condition (3) cannot be met. From the theoretical standpoint, the system is feasible even when $\alpha_s = \beta_p$. This obviously is a limit condition, while from the practical standpoint it is useful that $\alpha_s > \beta_p$, and that the ratio $\frac{\alpha_s}{\beta_p}$ is quite greater than one, such that the system remains feasible even when $\gamma^{(E)}$ has some fluctuations. In this work we neglect this fact, since we only consider static (or quasi-static) channels, and the only constraint we impose is $\alpha_s \geq \beta_p$. The ratio $\frac{\alpha_s}{\beta_p}$ will be studied in future works, where non-static channels will be considered as well.

When the system is feasible, i.e., the public message is more protected against noise than the secret one, and $\alpha_s \geq \beta_p$, we can compare different coding techniques by using the security gap S_g , defined as the ratio between Bob's minimum SNR and Eve's maximum SNR:

$$S_g = \frac{\beta_s}{\alpha_s}. \quad (4)$$

Obviously, the smaller the security gap, the better the system performance, since security can be achieved even with a small degradation of Eve's channel with respect to Bob's channel.

Based on the above considerations, the design target is to find codes which make the system feasible. In fact, differently from the wiretap channel model, in this case there is no guarantee that the system is feasible even when Eve has a degraded channel with respect to Bob. Then, a meaningful objective is to find codes able to achieve small security gaps. We will face these problems in the next sections.

B. Message concatenation and all-or-nothing transforms

In order to increase the difference between the two levels of protection against noise for the public and secret messages, we can resort to message concatenation [18] and all-or-nothing transforms (AONTs) [19]. Let us suppose that L secret messages, each with length k_s , are concatenated and then transformed through an AONT. The transformed string is then transmitted in L fragments, which replace the original messages. Only if all of them are correctly received, the AONT can be inverted and the L secret messages successfully obtained; otherwise, none of them can be even partially

recovered. Through concatenation, the error probability on each secret message becomes

$$P_s^{(L)}(\gamma) = 1 - [1 - P_s(\gamma)]^L \geq P_s(\gamma). \quad (5)$$

Hence, for a given $\gamma^{(E)} = \bar{\gamma}^{(E)}$, if $P_s(\bar{\gamma}^{(E)})$ does not meet the security condition, we can resort to message concatenation and AONTs, and find a suitable value of L such that $P_s^{(L)}(\bar{\gamma}^{(E)})$ overcomes the security threshold.

Obviously, when we introduce message concatenation and AONTs, we must replace $P_s(\gamma)$ with $P_s^{(L)}(\gamma)$ also for Bob. Hence, the use of these tools is paid in terms of the SNR working point for Bob, which increases with respect to the case without concatenation. In addition, increasing L increases the latency for receiving the secret message. Concerning the implementation of an AONT, several examples can be found in the literature. For the purposes of this study, we observe that scrambling the information bits through a linear (and dense) map can achieve features similar to those of an AONT, thanks to the randomness of the errors induced by the channel [18].

We note that AONTs can also be used, at higher layers, to achieve some desired level of computational security. In fact, the condition (1d) only guarantees that Eve's decoder has a high error probability on the secret blocks. However, this does not exclude that some secret blocks may be correctly decoded by Eve. Furthermore, even when Eve's decoder is in error, some bits within the block may be correct. Therefore, as often occurs in physical layer security, this setting represents a substrate which must be exploited by higher layer protocols to achieve some desired level of computational security.

III. USING TWO DIFFERENT LDPC CODES

Let us suppose to use two different LDPC codes to encode the public and the secret information blocks. For the sake of simplicity, our choice is to split the transmitted frame into two codewords of length $n/2$. One of these two codewords is obtained from an LDPC code C_p , having rate $R_c^{(p)}$, and carries the k_p public information bits. The other codeword belongs to an LDPC code C_s , with rate $R_c^{(s)}$ and corresponds to the k_s secret information bits. Since the two codes have the same length, provided that they are well designed, it must be $R_c^{(p)} < R_c^{(s)}$ to achieve a higher level of protection against noise for the public information block.

Example III.1 Let us consider $n = 2048$ and two LDPC codes with the following parameters:

- C_p : length 1024, rate $R_c^{(p)} = 0.2$.
- C_s : length 1024, rate $R_c^{(s)} = 0.8$.

Their variable and check node degree distributions have been optimized through the tools available in [20]. Concerning the choice of the node degrees, for the variable nodes we have used the same degrees we will consider in Example IV.1, while for the check nodes we have considered a concentrated distribution (i.e., with only two degrees, concentrated around the mean). The resulting variable and check node degree

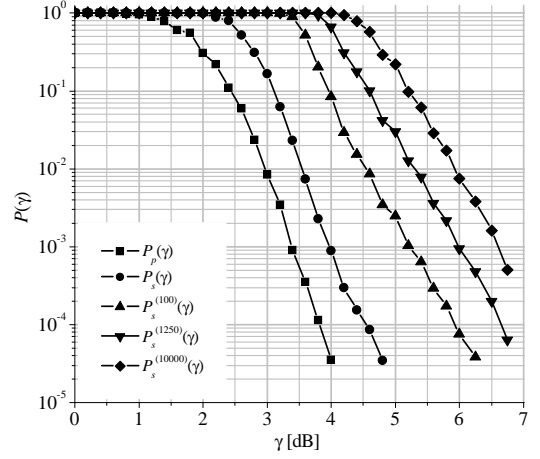


Fig. 2. Error rate curves for two different LDPC codes with length $n = 1024$ and rates $R_c^{(p)} = 0.2$, $R_c^{(s)} = 0.8$, with and without concatenation of the secret messages (indicated in the superscript of $P_s(\gamma)$).

distributions are, respectively,

$$\begin{aligned} \lambda(x) &= 0.1765x^{19} + 0.2392x^{18} + 0.0638x^{17} + 0.0988x^{16} \\ &\quad + 0.0117x^{15} + 0.1976x^2 + 0.2124x, \\ \rho(x) &= 0.1607x^6 + 0.8393x^5, \end{aligned} \quad (6)$$

for the first code, and

$$\begin{aligned} \lambda(x) &= 0.8815x^2 + 0.1185x, \\ \rho(x) &= 0.1708x^{14} + 0.8292x^{13}, \end{aligned} \quad (7)$$

for the second code. These degree distributions have been used to design the parity-check matrices of the two codes C_p and C_s through the *zigzag-random* construction [21], [22]. The performance of these codes, assessed through numerical simulations, and using the log-likelihood ratio sum product algorithm (LLR-SPA) with 100 maximum iterations for decoding, is reported in Fig. 2, also considering some examples of concatenation of the secret message ($L = 100, 1250, 10000$).

IV. USING UEP LDPC CODES

Let us suppose to use a single UEP LDPC code with length n . Most of the existing works on UEP LDPC codes aim at designing codes with three protection classes (PCs):

- PC1 contains $k_1 < k$ information bits which are those most protected against noise.
- PC2 contains $k_2 = k - k_1$ information bits which are less protected against noise than those in PC1.
- PC3 contains the whole redundancy part ($r = n - k$ bits).

Codes of this kind are suitable for the considered scenario. In fact, given an UEP LDPC code with the three PCs outlined above, we can map the public message bits into PC1 (i.e., $k_p = k_1$) and the secret message bits into PC2 (i.e., $k_s = k_2$).

To design LDPC codes with good UEP properties, several approaches have been proposed in the literature [22]–[24]. All these methods aim at optimizing the node degree distributions in such a way that the variable node degrees are spanned in a wide range, and good convergence thresholds are achieved under iterative decoding. Then the variable nodes with the

highest degrees are mapped into the bits of PC1, whereas the others form PC2 and PC3 (depending on their association with information or redundancy bits).

Once the variable node degree distribution $\lambda(x)$ has been designed, the number of bits in PC1 can be easily computed by converting $\lambda(x)$ from the edge perspective to the node perspective, the latter being expressed through another polynomial $\nu(x) = \sum_i \nu_i x^i$, and then computing the fraction of variable nodes with the highest degrees, that are those in PC1. We have

$$\nu_i = \frac{\lambda_i/i}{\sum_{j=1}^{\overline{d_v}} \lambda_j/j}, \quad \lambda_i = \frac{\nu_i \cdot i}{\sum_{j=1}^{\overline{d_v}} \nu_j \cdot j}, \quad (8)$$

where $\overline{d_v}$ denotes the maximum variable node degree. The same formulas can also be used for the check node degree distributions, by putting ρ in place of λ , c in place of ν and $\overline{d_c}$ in place of $\overline{d_v}$, where $\overline{d_c}$ is the maximum check node degree. Hence, $\rho(x)$ and $c(x)$ are the check node degree distributions from the edge and the node perspectives, respectively.

For the sake of simplicity, for the check node degrees we adopt a concentrated distribution, as already done in Section III for the case of different LDPC codes. Hence, we have

$$c(x) = ax^{\lfloor c_m \rfloor} + bx^{\lceil c_m \rceil}, \quad (9)$$

where $c_m = \frac{E}{r} = \frac{\sum_j v_j \cdot j}{(1-R)}$ and E is the total number of edges in the Tanner graph. The coefficients a and b are obtained as:

$$a = \lceil c_m \rceil - c_m, \quad b = c_m - \lfloor c_m \rfloor. \quad (10)$$

Example IV.1 Let us consider the following UEP LDPC variable node degree distribution taken from [24, Table 3], with some minor modifications to adapt the proportion between PC1 and PC2 in such a way that it coincides with the one used in Example III.1:

$$\begin{aligned} \lambda(x) = & 0.0025x^{19} + 0.0009x^{18} + 0.0031x^{17} + 0.0630x^{16} \\ & + 0.3893x^{15} + 0.2985x^2 + 0.2427x. \end{aligned} \quad (11)$$

The corresponding node perspective distribution is

$$\begin{aligned} \nu(x) = & 0.0005x^{20} + 0.0002x^{19} + 0.0007x^{18} + 0.0151x^{17} \\ & + 0.0835x^{16} + 0.4054x^3 + 0.4946x^2. \end{aligned} \quad (12)$$

The nodes in PC1 are those with degree ≥ 16 , while those with degree ≤ 3 are in PC2 or PC3 depending on their association to information bits or redundancy bits. This way, we find that PC1 and PC2 contain, respectively, 20% and 80% of the information bits. By using this distribution for the variable nodes and a concentrated degree distribution for the check nodes, we have designed three UEP LDPC codes with $n = 1024, 2048$ and 4096 . Their parity-check matrices have been obtained through the same zigzag random procedure used in Section III. The performance obtained by these codes under LLR-SPA decoding with 100 maximum iterations is reported in Figs. 3-5. Some examples of the use of concatenation of secret messages are also shown in Figs. 3 and 4.

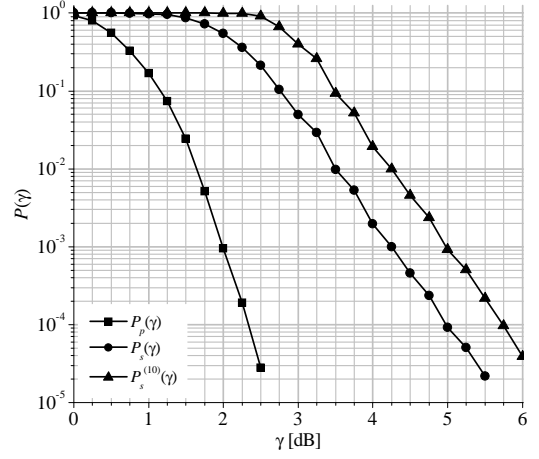


Fig. 3. Error rate curves for an UEP LDPC code with length $n = 1024$ and PC1 and PC2 with proportions 20% – 80%, with and without concatenation of secret messages (indicated in the superscript of $P_s(\gamma)$).

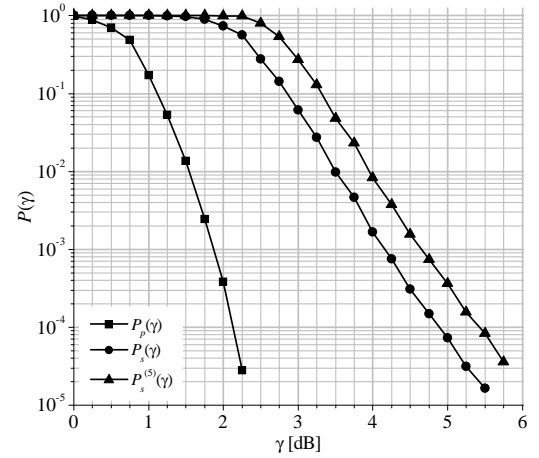


Fig. 4. Error rate curves for an UEP LDPC code with length $n = 2048$ and PC1 and PC2 with proportions 20% – 80%, with and without concatenation of secret messages (indicated in the superscript of $P_s(\gamma)$).

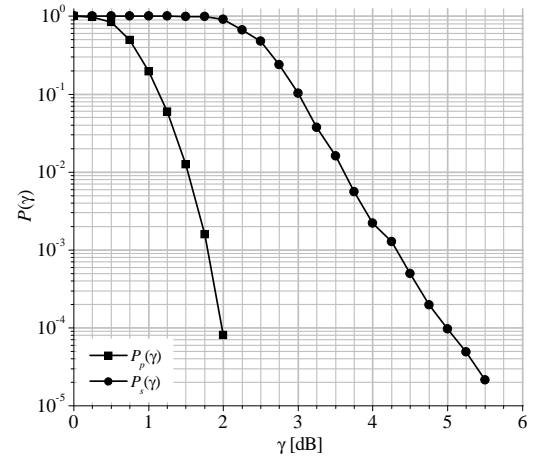


Fig. 5. Error rate curves for an UEP LDPC code with length $n = 4096$ and PC1 and PC2 with proportions 20% – 80%.

V. PERFORMANCE ASSESSMENT

We fix two values for the reliability and security thresholds, namely, $\delta = 10^{-4}$ and $\eta = 0.1$. Actually, one could think

TABLE I
PERFORMANCE ASSESSMENT OF THE CODING SCHEMES IN EXAMPLES
III.1 AND IV.1 ($\beta_p, \alpha_s, \beta_s$ AND S_g ARE IN dB) .

Scheme	n	L	β_p	α_s	β_s	S_g
UEP	1024	10	2.34	2.46	5.74	3.28
non-UEP	2048	1250	3.81	3.83	6.65	2.82
UEP	2048	5	2.13	2.37	5.43	3.06
UEP	4096	1	1.99	2.01	4.98	2.97

that a decoding error probability equal to 0.9 for Eve does not represent a condition of sufficient security. However, we remind that this setting only provides a substrate over which any desired level of computational security can be achieved through higher layer techniques, as described in Section II-B. Furthermore, our purpose is just to compare the considered coding schemes, not to define any absolute security level. For each coding scheme, we choose the smallest value of L such that the system is feasible, i.e., $\alpha_s \geq \beta_p$. Finally, we compute the values of β_s and the security gap S_g , according to (4).

The results obtained by considering the coding schemes in Examples III.1 and IV.1 are reported in Table I. From these examples, we observe that using UEP LDPC codes is actually effective for implementing practical transmission schemes over the BCC, since the system feasibility is achieved even with a small number of concatenated messages, and the security gap values are in the order of 3 – 3.3 dB. Increasing the block length improves performance: apart from a small reduction in the security gap, longer codes require a smaller SNR for Bob and less concatenation. In fact, while an UEP LDPC code with $n = 1024$ requires $L = 10$ and $\beta_s = 5.74$ dB, by increasing n to 4096 we reduce β_s to less than 5 dB (thus reducing Bob's SNR), and we no longer need the concatenation of secret messages for the system to be feasible. Instead, using two different codes is not a good choice, as we observe by comparing the second and the third rows of Table I. In fact, for $n = 2048$, the two non-UEP LDPC codes considered in Example III.1 achieve some small reduction in the security gap, but they require a very high level of concatenation ($L = 1250$) for the system to be feasible. This increases the minimum SNR for Bob by more than 1 dB, and also has detrimental effects on the system latency.

VI. CONCLUSION

We have studied the performance of some practical LDPC coded transmission schemes for the BCC. We have used the error rate as a metric, and proved that two different levels of protection against noise are needed for the public and the secret messages.

For this purpose, we have considered both UEP LDPC codes and classical non-UEP LDPC codes. We have considered some specific sets of parameters to provide some practical examples. For the considered cases, our results show that rather small security gaps can be achieved, and that using long UEP LDPC codes is advantageous, since it allows to avoid the use of message concatenation, thus reducing the required SNR and the transmission latency.

REFERENCES

- [1] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [3] M. van Dijk, "On a special class of broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 43, no. 2, pp. 712–714, Mar. 1997.
- [4] R. Liu and H. V. Poor, "Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages," *IEEE Trans. Inform. Theory*, vol. 55, no. 3, pp. 1235–1249, Mar. 2009.
- [5] Y.-K. Chia and A. El Gamal, "Three-receiver broadcast channels with common and confidential messages," *IEEE Trans. Inform. Theory*, vol. 58, no. 5, pp. 2748–2765, May 2012.
- [6] E. Ekrem and S. Ulukus, "Capacity region of Gaussian MIMO broadcast channels with common and confidential messages," *IEEE Trans. Inform. Theory*, vol. 58, no. 9, pp. 5669–5680, Sep. 2012.
- [7] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "New results on multiple-input multiple-output broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 59, no. 3, pp. 1346–1359, Mar. 2013.
- [8] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "The secrecy capacity region of the Gaussian MIMO broadcast channel," *IEEE Trans. Inform. Theory*, vol. 59, no. 5, pp. 2673–2682, May 2013.
- [9] R. F. Wyrembelski and H. Boche, "Physical layer integration of private, common, and confidential messages in bidirectional relay networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 9, pp. 3170–3179, Sep. 2012.
- [10] J.-C. Belfiore and F. Oggier, "Secrecy gain: a wiretap lattice code design," in *Proc. International Symposium on Information Theory and Its Applications (ISITA2010)*, Taichung, Taiwan, Oct. 2010, pp. 174–178.
- [11] H. Mahdavi and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," in *Proc. IEEE International Symposium on Information Theory (ISIT 2010)*, Austin, TX, Jun. 2010, pp. 913–917.
- [12] D. Kline, J. Ha, S. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the gaussian wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 532–540, Sep. 2011.
- [13] S. Watanabe and Y. Oohama, "Broadcast channels with confidential messages by randomness constrained stochastic encoder," in *Proc. IEEE International Symposium on Information Theory (ISIT 2012)*, Cambridge, MA, Jul. 2012, pp. 61–65.
- [14] M. Andersson, R. F. Schaefer, T. J. Oechtering, and M. Skoglund, "Polar coding for bidirectional broadcast channels with common and confidential messages," *IEEE J. Select. Areas Commun.*, vol. 31, no. 9, pp. 1901–1908, Sep. 2013.
- [15] C. W. Wong, T. F. Wong, and J. M. Shea, "Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 551–564, Sep. 2011.
- [16] M. Baldi, M. Bianchi, and F. Chiaraluce, "Non-systematic codes for physical layer security," in *Proc. IEEE Information Theory Workshop (ITW 2010)*, Dublin, Ireland, Aug. 2010.
- [17] —, "Increasing physical layer security through scrambled codes and ARQ," in *Proc. IEEE International Conference on Communications (ICC 2011)*, Kyoto, Japan, Jun. 2011.
- [18] —, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 883–894, Jun. 2012.
- [19] V. Boyko, "On the security properties of OAEP as an all-or-nothing transform," in *Advances in Cryptology – CRYPTO 99*, ser. Lecture Notes in Computer Science. Springer, 1999, vol. 1666, pp. 503–518.
- [20] (2013) LDPC codes project. University of Newcastle – Signal Processing Microelectronics research centre. [Online]. Available: <http://sigpromu.org/ldpc/>
- [21] X. Y. Hu, E. Eleftheriou, and D. M. Arnold, "Progressive edge-growth Tanner graphs," in *Proc. IEEE Global Telecommunications Conference (GLOBECOM'01)*, San Antonio, Texas, Nov. 2001, pp. 995–1001.
- [22] N. von Deetzen and S. Sandberg, "On the UEP capabilities of several LDPC construction algorithms," *IEEE Trans. Commun.*, vol. 58, no. 11, pp. 3041–3046, Nov. 2010.
- [23] H. V. B. Neto, W. Henkel, and V. C. da Rocha, "Multi-edge type unequal error protecting low-density parity-check codes," in *Proc. IEEE Information Theory Workshop (ITW 2011)*, Oct. 2011, pp. 335–339.
- [24] C. Poulliat, D. Declercq, and I. Fijalkow, "Enhancement of unequal error protection properties of LDPC codes," *EURASIP Journal on Wireless Communications and Networking*, vol. 2007, 2007, article ID 92659.